Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A cryptographic system for securing data on a computer network comprising:

a plurality of users coupled to the computer network; and

a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users, and each of the plurality of cryptographic devices comprising:

a processor programmed to authenticate ~~a~~ the plurality of remote users on the computer network for secure processing of a value bearing item (VBI);

a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users;

a cryptographic engine for cryptographically protecting data;

an interface for communicating with the computer network, and

a module for processing value for the value bearing item,

wherein ~~the plurality of cryptographic devices share a secret and~~ each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users, wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users, and

wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users.

2. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is programmed to verify that the identified user is authorized to assume a role and perform a corresponding operation.

3. (Currently Amended) The cryptographic ~~device~~ system of claim 2, wherein the assumed role is a key custodian role to take possession of shares of keys.

4. (Currently Amended) The cryptographic ~~device~~ system of claim 2, wherein the assumed role is an administrator role to manages a user access control database.

5. (Currently Amended) The cryptographic ~~device~~ system of claim 2, wherein the assumed role is a provider role to authorize increasing credit for a user account.

6. (Currently Amended) The cryptographic ~~device~~ system of claim 2, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

7. (Currently Amended) The cryptographic ~~device~~ system of claim 1 further comprising a stored secret for cryptographically protecting data.

8. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the secret is a password.

9. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the secret is a public/private key pair.

10. (Currently Amended) The cryptographic ~~device~~ system of claim 2, wherein the processor is programmed to include a state machine for determining a state corresponding to availability of commands in conjunction with the roles.

11. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is stateless.

12. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is programmed to prevent unauthorized and undetected modification of data.

13. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is programmed for preventing unauthorized disclosure of data.

14. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is programmed to ensure proper

operation of cryptographic security and VBI related meter functions.

15. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is programmed for providing indications of an operational state of a VBI meter.

16. (Currently Amended) The cryptographic ~~device~~ system of claim 2, wherein the processor is programmed for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

17. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor stores information about a number of last transactions in an internal register and compares the information saved in the register with the information saved in a memory before loading a new transaction data.

18. (Currently Amended) The cryptographic ~~device~~ system of claim 17, wherein the memory includes data for creating indicium, account maintenance, and revenue protection.

19. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item is a postage value including a postal indicium.

20. (Currently Amended) The cryptographic ~~device~~ system of claim 19, wherein the postal indicium comprises a digital signature.

21. (Currently Amended) The cryptographic ~~device~~ system of claim 19, wherein the postal indicium comprises a postage amount.

22. (Currently Amended) The cryptographic ~~device~~ system of claim 19, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

23. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item is a ticket.

24. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item includes a bar code.

25. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item is a coupon.

26. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item is currency.

27. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item is a voucher.

28. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the value bearing item is a traveler's check.

29. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

30. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices.

31. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the processor and the cryptographic engine generate a master key set (MKS).

32. (Currently Amended) The cryptographic ~~device~~ system of claim 31, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

33. (Currently Amended) The cryptographic ~~device~~ system of claim 32, wherein the MKS further includes a Master

Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

34. (Currently Amended) The cryptographic ~~device~~ system of claim 31, wherein the MKS is exported to other cryptographic devices.

35. (Currently Amended) The cryptographic ~~device~~ system of claim 1, further comprising a memory including a user profile for a subset of the plurality of users.

36. (Currently Amended) The cryptographic ~~device~~ system of claim 35, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period.

37. (Currently Amended) The cryptographic ~~device~~ system of claim 10, wherein the state machine comprises of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state.

38. (Currently Amended) The cryptographic ~~device~~ system of claim 37, wherein the operational state comprises means for access control, means for session management, and means for key management, and means for audit support.

39. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

40. (Currently Amended) The cryptographic ~~device~~ system of claim 1, wherein at least one of the plurality of users is an enterprise account.

41. (Currently Amended) A method for securing data on a computer network including a plurality of users and a plurality of cryptographic devices remote from the plurality of users, the method comprising the steps of:

authenticating any one of the plurality of remote users by any one of the plurality of cryptographic devices;

~~authenticating and~~ authorizing any one of the plurality of remote users for secure processing of a value bearing item by any one of ~~a~~ the plurality of cryptographic devices;

processing value for the value bearing item by ~~the~~ any one of the plurality of cryptographic devices; and

storing a security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is processed by any one of the plurality of cryptographic devices ~~related to the one of the plurality of users;~~

~~creating a secret by one of the plurality of cryptographic devices; and~~

~~exporting the created secret to the remaining of the plurality of cryptographic devices to be shared among the plurality of cryptographic devices;~~.

42. (Original) The method of claim 41 further comprising the step of printing the value bearing item.

43. (Original) The method of claim 41 further comprising the step of storing a plurality of security device transaction data in a database wherein, each transaction data is related to one of the plurality of users.

44. (Original) The method of claim 43 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item.

45. (Original) The method of claim 41 further comprising the steps of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation.

46. (Original) The method of claim 45, wherein the assumed role is an administrator role to manage a user access control.

47. (Original) The method of claim 45, wherein the assumed role is a provider role to authorize increasing credit for a user account.

48. (Original) The method of claim 45, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

49. (Original) The method of claim 45, wherein the assumed role is a security officer role for initiating key management function.

50. (Original) The method of claim 45, wherein the assumed role is a key custodian role to take possession of shares of keys.

51. (Original) The method of claim 45, wherein the assumed role is an auditor role to manage audit logs.

52. (Original) The method of claim 41, further comprising the step of printing a postage value including a postal indicium.

53. (Original) The method of claim 52, wherein the postal indicium comprises a digital signature.

54. (Original) The method of claim 52, wherein the postal indicium comprises a postage amount.

55. (Original) The method of claim 52, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

56. (Original) The method of claim 41, further comprising the step of printing a ticket.

57. (Original) The method of claim 41, further comprising the step of printing a bar code.

58. (Original) The method of claim 41, further comprising the step of printing a coupon.

59. (Original) The method of claim 41, further comprising the step of printing a currency.

60. (Original) The method of claim 41, further comprising the step of printing a traveler's check.

61. (Original) The method of claim 41, further comprising the step of printing a voucher.

62. (Original) The method of claim 41, further comprising the step of storing a user profile for a subset of the plurality of users.

63. (Original) The method of claim 62, wherein the user profile includes username, user role, password, logon

failure count, Logon failure limit, logon time-out limit, account expiration, password expiration, and password period

64. (Original) The method of claim 41, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms by each of the cryptographic devices.

65. (Original) The method of claim 41, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.

66. (Original) The method of claim 41, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database; and

comparing the information saved in the respective device with the respective information saved in the database.

67. (Original) The method of claim 66, further comprising the step of loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

68. (Original) The method of claim 41, wherein the secret is a password.

69. (Original) The method of claim 41, wherein the secret is a public/private key pair.

70. (Original) The method of claim 41, wherein at least one of the plurality of users is an enterprise account.

71. (New) The method of claim 41, wherein the security device transaction data is related to user authorization operations, user account operations, and VBI creation operations, and wherein each of the user authorization operations, user account operations, and VBI creation operations can be performed by any one of the plurality of cryptographic devices.